CHAPTER

7

SECURING NETWORK COMMUNICATIONS

After reading this chapter and completing the exercises you will be able to:

- Plan a secure network communication implementation by using Server Message Block signing.
- Plan and implement secure network transmission by implementing IP Security.

Many corporations spend a large amount of time and use a variety of technologies to make access to network resources and services secure. One potential security risk that is often overlooked is network communication or the actual transmission of the data across the network. For example, a company may implement a highly secure area for printers that print confidential information. Such printers are often locked in a specific room accessible only by authorized users. This environment may provide security for the printed documents, but does not secure the actual transmission of the data to the printer itself. An unauthorized user, with the appropriate network sniffer utility, could potentially capture the printing transmission and read the contents of the capture.

As stated in Chapter 1, "Identifying Security Risks," there are many types of potential attacks that could be applied to transmitted data. One of the more serious threats involves the active attack of capturing data being transmitted, altering the contents, and then sending the data to its intended destination. This could be accomplished by performing a man-in-the-middle attack. The attacker can capture all communication between the client and server, modify the information, and then resend the data without the victims knowing that anything has been changed.

Another threat is the transmission of passwords across the network. Many services, such as telnet applications or even some e-mail applications or Web browsers transmit passwords as clear text. There are many utilities available that allow an attacker to capture the logon traffic and easily read the password of the user logging onto the network service.

For some environments, these risks must be overcome by implementing security on the transmission of data between client and destination. Two main methods can be used to provide this protection: Server Message Block signing and IP Security.

Server Message Block (SMB) signing helps to insure that a client is connecting to the correct server, and not an attacker's computer posing as a server. As well, SMB signing can also be used to insure the server's trust of the client machine. **IP Security (IPSec)** provides the authentication security of SMB signing, but also encrypts that data between two points. This chapter contains information on the theory, implementation, and security design concepts to be considered when planning for the use of SMB signing or IP Security.

Implementing Server Message Block Signing

SMB signing is a protocol used between computers to share resources such as files, printers, and communication connections, including named pipes and mail slots. This protocol is also known as the Common Internet File System (CIFS). SMB signing refers to two main functions:

- *Message Authentication*—The ability to digitally sign each message block that is sent between a server and client. Each digital signature makes certain that the message blocks are not changed in transit between a client and a server.
- *Mutual Authentication between the server and client*—This insures that the client is connecting to the proper server, and the server is connecting to the original client and not to an imposter on either end.

SMB signing is usually implemented in environments that have a high security need to insure the validity of the client and server transmissions within the internal network. IP Security can also be used for this purpose, but it is only supported by Windows 2000 clients. One main advantage to SMB signing is that it can be incorporated within a multiclient environment. Windows 2000, Windows NT (SP3 or later), and Windows 98 clients can all take advantage of the increased security provided by SMB signing.

One of the issues that you will need to plan for is that SMB signing decreases CPU performance on a machine by 10-15% because of the increased overhead in signing and verifying each message block. On a busy file server, this can cause a significant decrease in file transfer performance.

Configuring SMB Security

SMB signing is implemented by editing a registry setting on each machine that is to be secured. Depending on the operating system, the registry setting can be deployed in a number of ways.

Manually Editing the Registry

The first option to enable SMB signing is to manually edit the registry on all computers. To manually configure SMB signing on a Windows 2000 server, follow the procedure below:

1. Click **Start**, click **Run**, and type **Regedt32** to open the Registry Editor.
2. Browse to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters.
3. Look for (or add) a REG_DWORD value called enablesecuritysignature. Enter a value of 1 to enable SMB signing. A value of 0 disables SMB signing. If you configure a server to enable SMB signing, it will attempt to establish the secure connection with all clients, but will accept nonsecure transmissions (for example, with a client that has not been enabled for SMB signing).
4. To require SMB message signing for clients to be able to connect to this server, add a REG_DWORD value called **requiresecuritysignature**. A value of 1 enables this requirement, and a value of 0 disables this requirement. Servers that are configured to require SMB signing will not accept connections from clients that do not support SMB signing.

Figure 7-1 illustrates the two SMB signing registry settings.

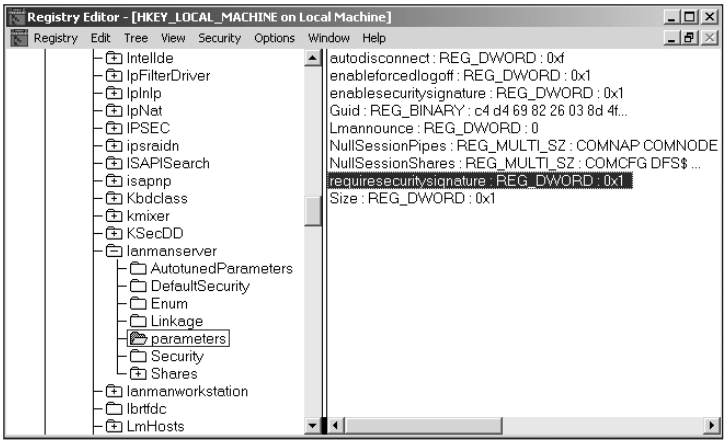

Figure 7-1 Editing SMB configuration settings within the Registry

To manually edit the Registry settings on a Windows 2000 client, edit the values as stated below:

- *Key*: HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\
  - Value: EnableSecuritySignature

  - Date Type: REG_DWORD
  - Value: 0 (disabled), 1 (enabled)
- *Key*: HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\
  - Value: RequireSecuritySignature
  - Date Type: REG_DWORD
  - Value: 0 (disabled), 1 (enabled)

Windows NT servers and clients support SMB signing as long as Service Pack 3 or above has been installed. To manually edit the Registry values on a Windows NT client, edit these values:

- *Key*: HKLM\System\CurrentControlSet\Services\Rdr\Parameters\
  - Value: EnableSecuritySignature
  - Date Type: REG_DWORD
  - Value: 0 (disabled), 1 (enabled)—enabled by default
- *Key*: HKLM\System\CurrentControlSet\Services\Rdr\Parameters\
  - Value: RequireSecuritySignature
  - Date Type: REG_DWORD
  - Value: 0 (disabled), 1 (enabled)

Windows 98 clients can also participate in SMB signing with a Windows 2000 server. To enable SMB signing on a Windows 98 client, manually edit the Registry by adding or modifying the following values:

- *Key*: HKLM\System\CurrentControlSet\Services\VxD\Vnetsup\
  - Value: EnableSecuritySignature
  - Date Type: REG_DWORD
  - Value: 0 (disabled), 1 (enabled)—enabled by default
- *Key*: HKLM\System\CurrentControlSet\Services\VxD\Vnetsup\
  - Value: RequireSecuritySignature
  - Date Type: REG_DWORD
  - Value: 0 (disabled), 1 (enabled)

In all cases, a reboot is required for any Registry changes to take effect.

Creating and Deploying Registry Files

Manually modifying the Registry on a large number of servers and workstations requires a great deal of administrative effort. An easier option to modify the Registry on a large number of computers is to create a Registry file, and then automate the process of importing the Registry changes into the client registries. In this way, Registry files can be used to deploy configuration settings to the workstations on the network. If you are going to use this method, be sure to create the Registry file using the same operating system as the workstations are using. For example, if a Registry file is created using Windows 98, do not import the configuration setting onto a Windows 95 client. Windows 95 clients do not support SMB signing. As well, do not import a Registry file from a Windows 2000 computer into the Registry on a Windows 98 or Windows NT computer.

To create a Registry configuration file, follow the steps below:

1. Click **Start**, click **Run**, and type **regedit** to start the Registry editor.
2. Depending on the operating system used, browse to and select the appropriate path within HKEY_LOCAL_MACHINE, as identified earlier.
3. Modify the Registry settings to enable SMB signing or to require SMB signing.
4. Click **Registry** and choose **Export Registry File**. See Figure 7-2. Save the selected Registry branch with an appropriate name and location.

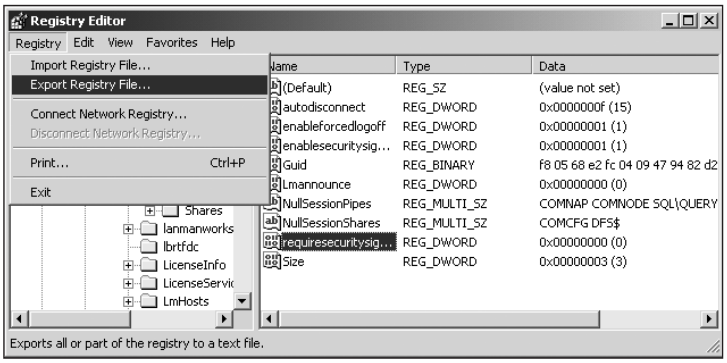

Figure 7-2 Saving a configured Registry file

This Registry file can then be distributed to the client workstations on the network. In most situations, the easiest way to do this is to e-mail the files to the appropriate clients and instruct the users to double-click the .reg file to import the changes into the Registry. In other situations, you may want to modify the user logon script to import the Registry changes.

Modifying the Registry with a .reg file can have serious consequences if the Registry changes have not been tested. Before deploying this .reg file into the production environment, test it thoroughly.

Windows 2000 Group Policy

The third option for implementing SMB signing is to use group policies. This is the easiest way to deploy and maintain the SMB signing configuration with Windows 2000-based machines. In a domain environment, SMB configuration settings can be stored in a security template and deployed at a site, domain, or organizational unit level.

To configure a security template to apply SMB signing, follow the steps below:

1. Click **Start**, and then click **Run**.
2. Type **mmc** in the Run command line. An empty MMC will appear. You may want to maximize the console.
3. Click the **Console** menu and click **Add/Remove Snap-in**.
4. Click the **Add** button.
5. In the Add Standalone Snap-in dialog box, scroll down and click **Security Templates**, and then click the **Add** button.
6. Click **Close**, and then click **OK**.
7. Expand the **plus sign** next to Security Templates in the left pane.
8. The next node will show you the physical location of the security template files on the server. The location of the template files is usually c:\%systemroot%\security\templates.
9. To save the new MMC, click **File** and click **Save As**. Choose an appropriate name and location for the MMC console file.
10. Create a new template file by right-clicking the security template path in the left pane and clicking **New Template**. Type a name and description in the dialog box.
11. Select the new template, and browse to the **Local Policies\Security Options** node.
12. Scroll to the SMB signing configuration settings and enable the required options as shown in Figure 7-3.
13. Save the settings by right-clicking the template and clicking **Save**.

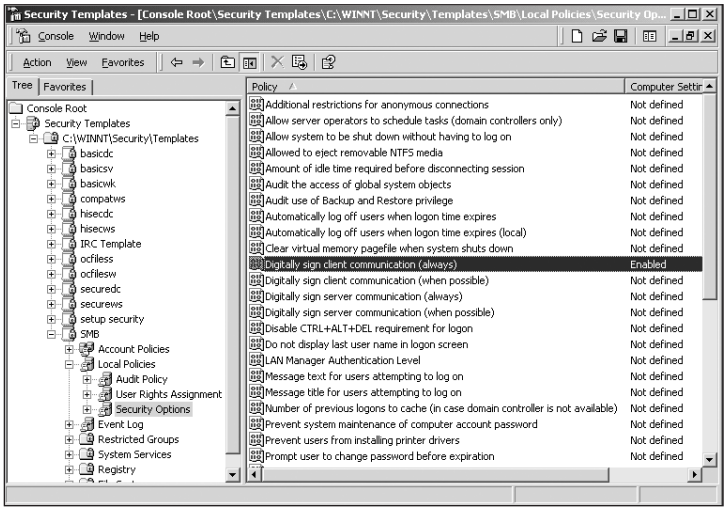

Figure 7-3 Configuring SMB digital signing using a security template

There are four SMB signing security options available in the template:

- *Digitally sign client communications (always)*—Requires the Windows 2000 client to use SMB signing during a session.
- *Digitally sign client communications (when possible)*—The Windows 2000 client requests SMB signing but will fall back to normal if the request is not granted.
- *Digitally sign server communications (always)*—Requires a Windows 2000 server to use SMB signing during a session.
- *Digitally sign server communications (when possible)*—The Windows 2000 server asks a client to communicate with SMB signing but will allow normal communication if the client is not configured appropriately.

Once the template is complete, it can be imported into a group policy object at the site, domain, or organizational unit level. The new SMB signing configuration will be applied the next time the group policy is refreshed on the computers in the Active Directory container.

Securing Network Traffic Using IP Security

The first step in securing the network traffic in your corporation is to limit which users can log on to your network. Kerberos is effective in controlling user access to the network by enforcing and protecting the authentication of users. Many corporations also have strict policies preventing any users, such as consultants from outside the corporation, from connecting their computers to the network. If a user were to gain access to

the network, he could capture any packet on the network and read its contents because, by default, much of the data on a network is passed in clear text. For network environments where higher levels of security are needed, or where part of the network is exposed to the Internet, passing data in clear text may be an unacceptable risk. IPSec, which is a protocol used for data authentication and encryption over a network, is a solution to this problem.

With IPSec, all the data that is transmitted on a network can be encrypted. The encryption takes place at the IP network layer, which means that the encryption is invisible to both the applications at higher levels of the TCP/IP stack and to the lower physical layers. Applications do not need to be IPSec-aware because when the data is passed to the application, it is no longer encrypted. At the lower physical layers, the data is encrypted, but these layers see the data only as a packet that must be delivered to a destination without any need to see the contents of the packet. The fact that the use of IPSec is transparent to the applications (and the users) is one of the biggest advantages of IPSec. You can configure all or some of the computers on your network to use IPSec, and you do not have to change any applications or settings on your network.

In addition to encryption, IPSec provides further protection by supporting authentication methods to verify the sender and receiver of the data. Authentication can take place using such methods as Kerberos, certificates, or a shared password.

The Windows 2000 implementation of IPSec is flexible, easy to administer, and completely transparent to the user. Different computers on a network may need more or less security. For example, the server where highly confidential financial data is kept will need much more security than the server where publicly available information for customers is stored. By grouping these servers into separate organizational units, and then applying different IPSec configurations through Group Policy at the OU level, you can centrally configure and manage the IPSec settings for your entire organization.

IPSec consists of two protocols that can be used either independently or together to protect data: Authentication Header Protocol (AH) and Encapsulating Security Payload (ESP).

Authentication Header Protocol

The **Authentication Header Protocol (AH)** provides data authentication, integrity, and anti-replay protection for the data transmitted over the connection. AH, by itself, does not encrypt any portion of the packet. If a packet protected by an Authentication Header is captured, the IP header and data can be read, but cannot be modified without the recipient being aware of the change. As shown in Figure 7-4, the authentication header is placed right after the original IP header, but before the TCP/UDP header. This authentication portion is used to verify the integrity of the packet when it reaches its destination.

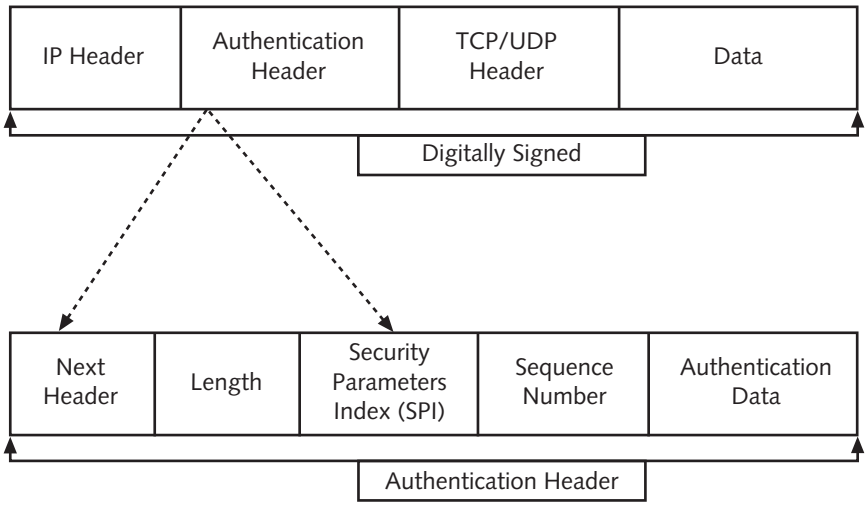

Figure 7-4 The IPSec Authentication Header packet structure

The expanded portion of the Authentication Header in Figure 7-4 illustrates the various sections of the Authentication Header itself. The header is composed of the following sections:

- *Next Header*—The protocol ID of the next header in the packet. For example, for TCP, the next header value would be six. This header indicates that the actual data in the packet is in a TCP packet.
- *Length*—The length of the AH header.
- *Security Parameters Index (SPI)*—Identifies the security association for this packet. The security association was negotiated during the ISAKMP protocol exchange between the source and destination. (The process of negotiating the security association will be discussed later.)
- *Sequence Number*—A 32-bit number that identifies the order in which each packet is issued for a specific security association. This number is used to protect against anti-reply attacks. The sequence number is compared to a list of previously received packets for this Security Association connection. If the sequence number has already been received, the packet is assumed to be invalid and is rejected.
- *Authentication Data*—The hash value calculated against the signed portion of the AH packet. The hash value is calculated by applying a mathematical formula to the content of the packet.

When the destination computer receives the packet, it checks the integrity and authenticity of the packet by calculating its own hash value and comparing it to the one stored in the Authentication Data portion of the header. If the values match, the packet is accepted; if the values do not match, the packet is discarded.

AH is supported only by Windows 2000 machines. If mutual authentication is needed in a mixed environment, use SMB signing.

Encapsulating Security Payload

Encapsulating Security Payload (ESP), similar to Authentication Headers, provides authentication, integrity, and anti-replay protection. In addition to these security features, ESP also provides data encryption capabilities. ESP can be used in addition to, or instead of, Authentication Headers. The main reason for using both ESP and AH is that AH protects the entire packet from modification, whereas ESP protects only the TCP/UDP header and the IP data payload.

An ESP packet inserts an ESP header between the original IP header and the TCP/UDP header, and also includes an ESP trailer to indicate the end of the encrypted data. Figure 7-5 illustrates the ESP protected packet.

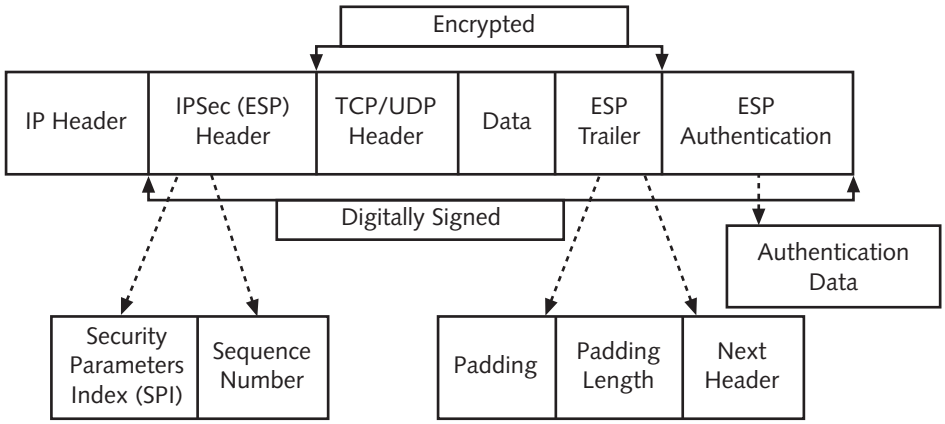

Figure 7-5 The IPSec Encapsulating Security Payload packet structure

The ESP header includes the Security Parameters Index (SPI) and Sequence Number fields that perform the same job as the corresponding AH header fields. The ESP trailer consists of the following sections:

- *Padding*—A variable length field used to adjust the length of the application data and ESP trailer to match the required size for the cipher algorithm.
- *Padding Length*—Indicates the length of the padding field.
- *Next Header*—Indicates the protocol used for the transmission of the data, for example TCP or UDP.
- *Authentication Data*—The field containing the hash checksum used to digitally sign the packet.

As you prepare your security plan to protect network traffic, one of the issues that you will have to plan for is which IPSec protocol or protocols you need to use. If the security plan requires that only authorized users are able to connect to a server using a specific protocol, IPSec Authentication Headers may be the answer. If data transmitted between two machines requires encryption, ESP will be the protocol of choice. For full protection and the benefit of IPSec, both can be implemented together.

IPSec can pass through a firewall as long as the firewall rules are set to allow UDP 500, Protocol ID 51 (AH), and Protocol ID 50 (ESP).

IPSec Modes

The last section described the two protocols available when deploying IPSec. Another decision that you will need to make is which IPSec mode you need to deploy. You can deploy IPSec by using one of two modes: Transport mode or Tunnel mode. **Transport mode** is used when you want to protect the network traffic from end to end, that is, from the client computer to the server. **Tunnel mode** can be used when only part of the connection from the client to the server needs to be protected. For example, if the traffic from client to server crosses an internal LAN segment, then goes through the Internet to another internal LAN segment, you may want to protect the traffic only when it is being sent across the Internet.

Transport Mode

Transport mode is implemented when communications need to be encrypted from an originating point through to a target point. Using AH, ESP, or a combination of the two, all data can be protected for the entire transmission between the two hosts. In transport mode, only the two end systems need to support IPSec; the connections between the two systems forward only the packets. In other words, if you want to protect all the data flowing from a single client computer to a specific server, you can configure those two computers and do not have to modify any settings on any other computers or networking devices. The only disadvantage with transport mode is that communication cannot take place through a Network Address Translation (NAT) firewall, because the IP addresses that are translated by the NAT device are protected by IPSec.

Figure 7-6 illustrates Transport mode from the client computer to the server. The router is used to forward the packets; it does not need to support IPSec.

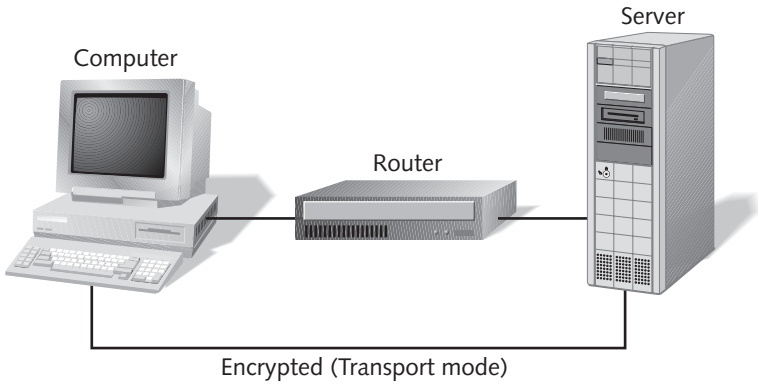

Figure 7-6 A client and server exchanging data using Transport mode

Tunnel Mode

Tunnel mode encrypts transmitted data between two points in a communication channel, thus forming a protected "tunnel" for only part of the channel. In this mode, when a client sends data to a server, the data is initially unprotected until it reaches the start of the tunnel. The data is then protected from the start of the tunnel to the tunnel end point. The data is then unprotected again as it is sent to the final destination computer. Figure 7-7 illustrates how IPSec Tunnel mode protects data between the routers, although the data is unprotected outside of the tunnel.

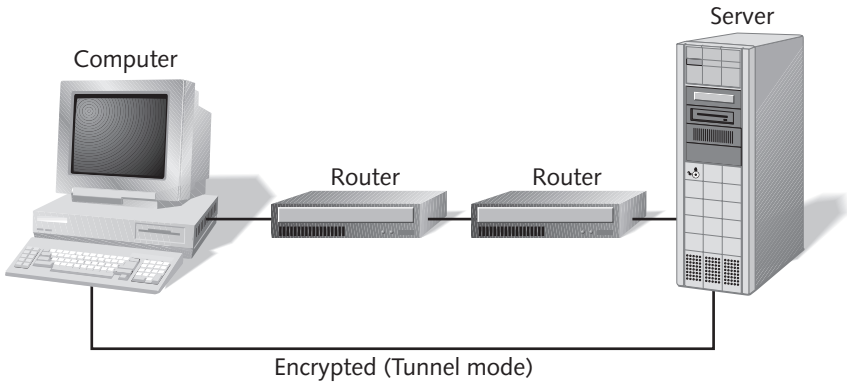

Figure 7-7 A client and server exchanging data using Tunnel mode

Tunnel mode is usually deployed between routers connecting a main office and a remote office over a WAN link. This connection may be a VPN connection over the Internet, which is protected by the IPSec tunnel. Tunnel mode is used if data must be protected on the Internet WAN connection, but does not need to be encrypted within the private networks behind the router.

IPSec with Windows 2000

Windows 2000 implements IPSec by utilizing various components that can be used to create, configure, and maintain security policies. These components include:

- *IPSec Policy Settings*—You can use the IPSec Policy Settings to decide what types of communication protocols are permitted or denied, the IPSec configuration for different computers, and the type of protection that is required (AH or ESP).
- *IPSec Policy Snap-In*—A custom IPSec console can be created to configure and apply IPSec-related policies.
- *IPSec Policy Agent Service*—This service is installed on each system configured with IPSec. The Policy Agent accesses the policy information stored in Active Directory and forwards the information to the IPSec driver.
- **Internet Key Exchange (IKE)**—Manages Security Associations, and generates and manages the exchange of the keys between the two systems.
- **IPSec driver**—Receives the filter list from the IPSec Policy configured on the machine. The filter list defines what type of traffic must be protected with IPSec. The IPSec driver also is in charge of the IKE to make sure that the key exchange process is taking place between the two machines.

When two computers need to exchange information and they are configured to use IPSec, a number of steps occur before the actual exchange of information. In Figure 7-8 and the following steps, assume that Computer A is sending information to Computer B and that an IPSec policy has been configured on both machines.

1. The IPSec driver on Computer A intercepts the packet and compares the message's destination IP address or protocol with the IPSec Policy Settings configured on the computer, checking to see whether a policy has been configured that indicates that the data being sent to Computer B should be protected.
2. If there is a match between the message and the filter, then Computer A's IPSec driver instructs the Internet Key Exchange (IKE) to begin a negotiation and creation of a **Security Association (SA)** with Computer B. IKE is also known as the Internet Security Association and Key Management Protocol (ISAKMP). This first negotiation is for the purpose of negotiating a secret key that will then be used to exchange the actual key used to encrypt the data. In this negotiation, the computers compare the different levels of encryption that both are capable of and choose the most secure common option.
3. Using the secret key, the computers now negotiate a second Security Association (SA) to determine what level of encryption to use for the data encryption and to exchange a key to use for the encryption. The results of the SA are returned to the IPSec driver.

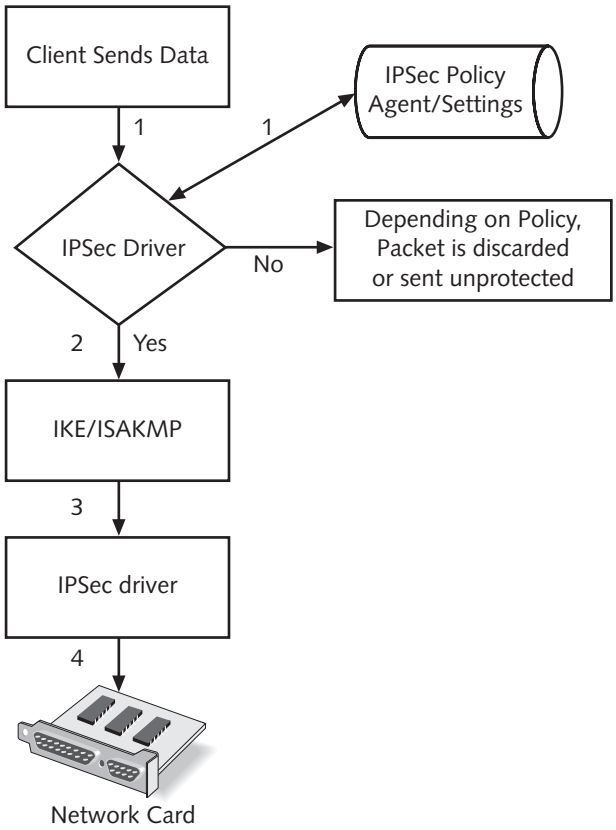

Figure 7-8 The IPSec negotiation process

4. The IPSec driver on Computer A encrypts and signs the packets and sends the packets down to the network card for transmission to Computer B.
5. Computer B receives the packets, sends the packets to its IPSec driver, which decrypts and verifies the integrity of the packet using the shared key. The IPSec driver then sends the packet to the correct application.

Encrypting and decrypting packets can be processor-intensive. To increase the server performance, consider purchasing IPSec-enabled network cards that offload the encryption/decryption process to the network card.

IPSec Policy Configuration

One of the features of IPSec in Windows 2000 is that you can manage the IPSec configuration for your entire network through Group Policies. To implement IPSec, you can create the policies that match the various IPSec requirements that you have on your network, and then link the policies to the Active Directory containers containing the computer

objects. The first step in creating an IPSec policy is to define the IP filters that you will need. The IP filters define the following characteristics:

- *Source or Destination IP Address*—You can define whether to apply the IPSec policy to a specific IP address or to an entire subnet, which means that you can protect the traffic between two specific computers or all the computers on a subnet.
- *Protocol Type*—You can define which traffic will be protected based on the protocol or protocol ID used in the transmission. For example, you may want to encrypt only SMTP traffic and not protect traffic using any other protocol.
- *Source or Destination Protocol Port*—You can also define which traffic will be protected based on the port number used by the protocol to communicate.

To configure IPSec and create the IP filters, follow the steps below:

1. Create a custom MMC console with the IP Security Policy Management Snap-in.
2. Right-click the **IP Security Policies** node in the left pane and choose **Manage IP filter lists and filter actions** from the shortcut menu. The configuration interface is shown in Figure 7-9.

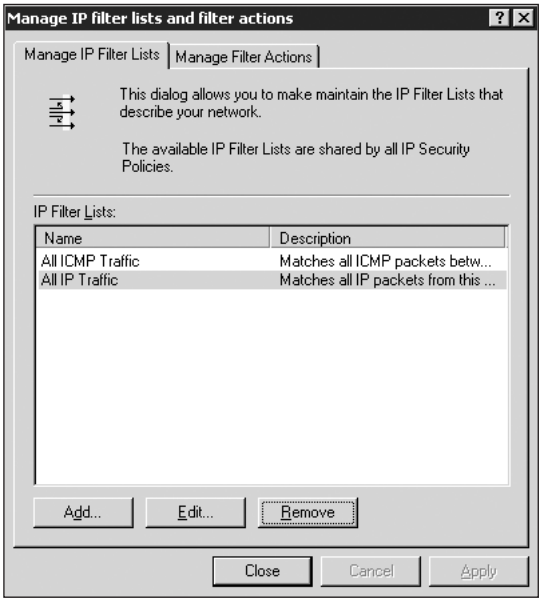

Figure 7-9 The Manage IP filter lists and filter actions dialog box

3. Click **Add** to add a new IP filter to the list. The Use Add Wizard starts automatically. (For these steps, the Wizard will be turned off by clearing the Use Add Wizard check box.)

4. Click **Add** to configure the new filter properties as shown in Figure 7-10.

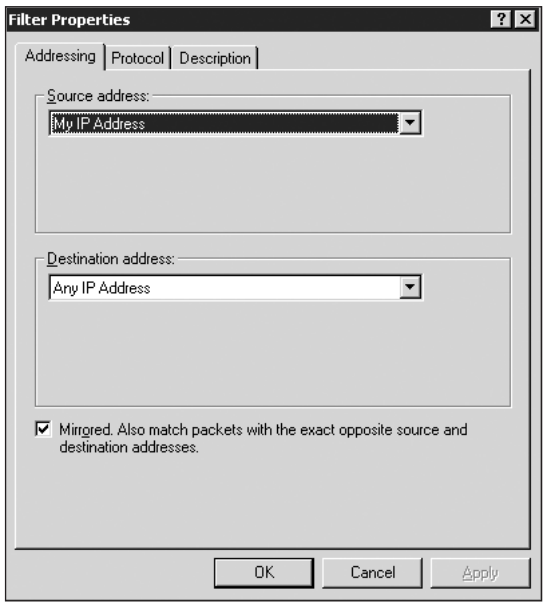

Figure 7-10 Configuring Filter Properties

5. Configure the Addressing and Protocol tabs as needed. On the Addressing tab, you can configure the IP addresses or DNS name that fall under this IPSec filter. On the Protocol tab, you can configure which protocols (based on protocol name, protocol number, or port number) will be included in this filter. To insure that the traffic is protected in both directions, check the **Mirrored** check box.

As shown in Figure 7-9, there are two default filters created on a Windows 2000 computer. These default filters apply to all IP traffic and all ICMP traffic. Additional filters are usually created to restrict transmissions between specific machines within a network or to protect traffic using a specific protocol. For example, if the Accounting department needed to have protected communication to the Accounting server, an IP filter could be created that defined the Accounting department computers as the source IP address and the Accounting server as the destination IP address. Or, if you want to make sure that all traffic between Exchange 2000 servers is encrypted, you could create an IPSec filter to encrypt all SMTP traffic.

The second step in the IPSec policy creation process is to define the actions that will take place if a client sends a packet that matches the filters. To create or edit filter actions, follow the steps below:

1. In the IP Security Policies console, right-click the **IP Security Policies** node in the left pane.

2. Choose **Manage IP filter lists and filter actions** from the shortcut menu.
3. Click the **Manage Filter Actions** tab. The interface is shown in Figure 7-11. There are three default filter actions available for use:
   a. *Permit*—Permits unsecured packets to pass through the filter.
   b. *Request Security (Optional)*—Requests an IPSec negotiation, but will accept communication with machines that do not support IPSec.
   c. *Require Security*—Requests an IPSec negotiation, but will allow communication only with machines that are IPSec enabled.

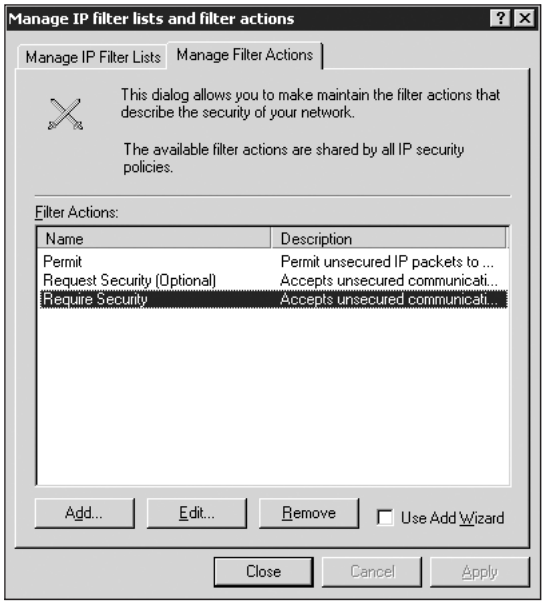

Figure 7-11 Creating or editing Filter Actions

4. To create a new action, click the **Add** button. To edit a default action, click **Edit.** The interface is shown in Figure 7-12.

As shown in Figure 7-12, you have three options when configuring the filter action:

- *Permit*—This selection allows packets through without IPSec protection.
- *Block*—If this action is applied to a specific filter, it will block transmission of any packets that match the filter.
- *Negotiate security*—This selection allows the administrator to be specific about which encryption and hash algorithms will be used to secure data transmission if the filter matches the data type being transmitted.

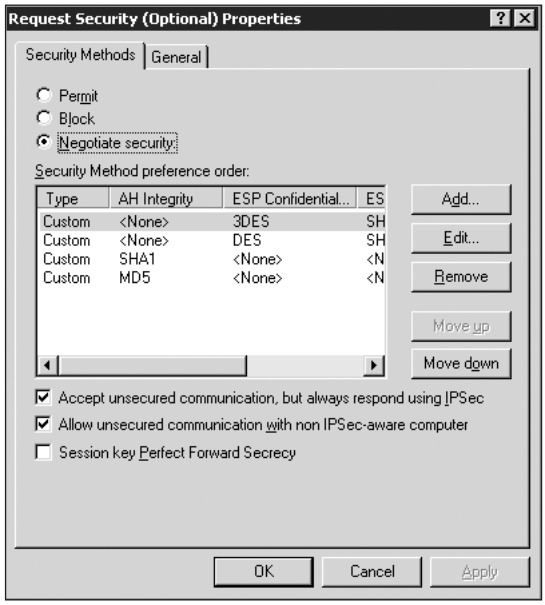

Figure 7-12 Editing a default IPSec action

The third step in configuring the IPSec policies is to determine the type of authentication that will take place between two network hosts before they take part in Security Association negotiations. Windows 2000 IPSec provides three ways to authenticate between the two machines involved:

- *Kerberos*—This is the default authentication protocol in Windows 2000. All Windows 2000-based computers can support this type of authentication. The main disadvantage is that this method cannot be used between Active Directory forests or with computers that are not in an Active Directory domain.
- *Certificates*—Mainly used in organizations that have a Public Key Infrastructure in place. This authentication method is convenient for integrating clients between separate enterprise networks.
- *Preshared Keys*—These are text strings or shared passwords entered into the IPSec configuration settings on both hosts. This is usually implemented only in a test environment, or when the other two authentication methods are not available.

The authentication method is configured during the creation or editing of the IP Security Policy. The creation of the policy is discussed in the following section.

IPSec Policy Creation

Once the policy elements, such as filters and actions, have been created, the actual IPSec policy can be created based upon the preconfigured elements.

To create the IPSec policy, follow the steps below:

1. Create a custom MMC console with the IP Security Policy Management snap-in.
2. Right-click the **IP Security Policies** node in the left pane and click **Create IP Security Policy**.
3. The IP Security Policy Wizard starts. Click the **Next** button.
4. Give the new policy a name and description. Click **Next**.
5. Choose to activate the default response rule. Click **Next**.
6. Select the Authentication method required for the default response rule. The three choices are illustrated in Figure 7-13. Click **Next**, and then click **Finish**.

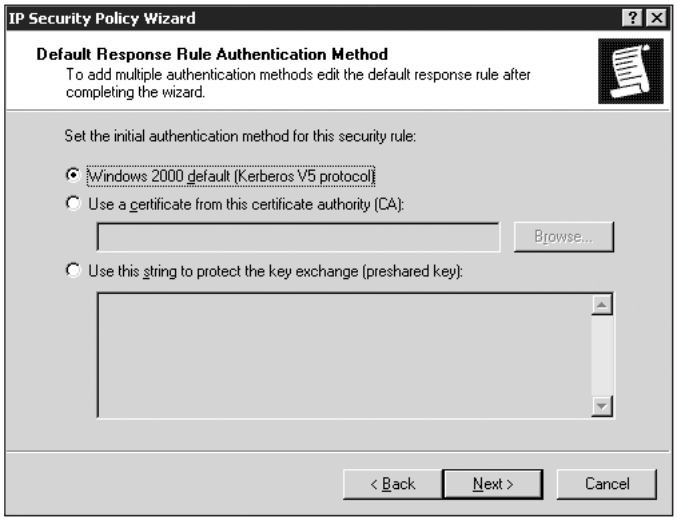

Figure 7-13 Selecting the default response rule authentication method

7. The new policy properties dialog box appears, with the default rule already configured. To add a new rule, click **Add**. The interface is shown in Figure 7-14.

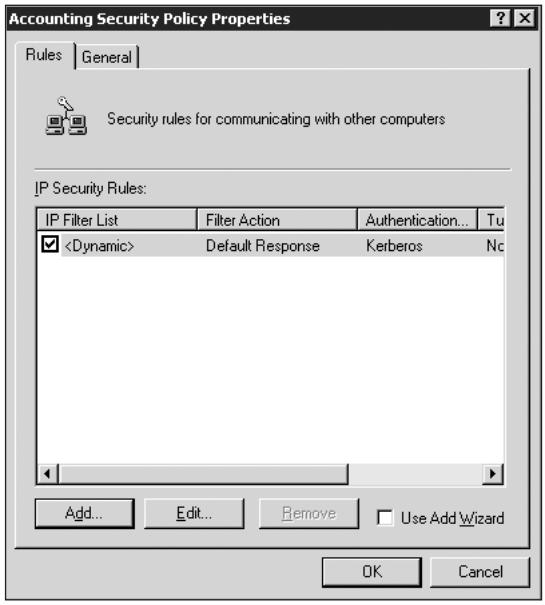

Figure 7-14 Creating new rules for IPSec policies

8. The new rule properties (as shown in Figure 7-15) present you with the choices of IP Filters, Actions, Authentication Methods, Tunnel Type, and the type of connections that this rule will be used for. Click **OK** to finish the configuration.

IPSec Deployment

IPSec policies can be configured and deployed on a local computer or, more frequently, are configured using the IP Security snap-in and then assigned to a Group Policy object in Active Directory.

After you have configured all of the policies that are required for your network, you can assign them to a local computer by following the steps below:

1. To open the TCP/IP properties page, right-click **My Network Places** and click **Properties**. Right-click **Local Area Connection,** click **Properties**, and then select **Internet Protocol** and click **Properties.**
2. Click **Advanced,** then click the **Options** tab and select **IP security**. Click **Properties**.
3. In addition to the custom policies that you have created, there are three default policies available for the computer:
   a. *Client (Respond Only)*—With this setting, the computer will listen for IPSec requests coming from other computers and respond by using IPSec; however, the computer will never initiate an IPSec connection.

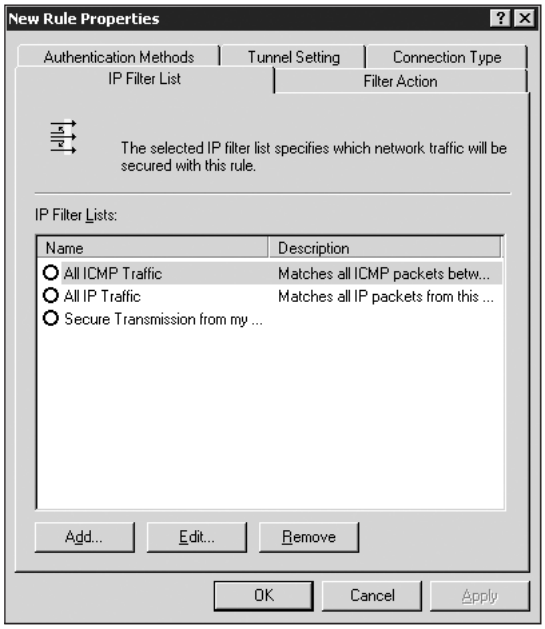

Figure 7-15 Configuring new rule properties

b. *Server (Request Security)*—The computer will always try to request IPSec connections with all computers that connect to it. However, if the other computer does not support IPSec, the server will accept connections that are not encrypted.

c. *Secure Server (Require Security)*—The computer will not accept any connections that are not encrypted using IPSec.

4. Choose the desired setting and click **OK.**

Administering the IPSec policy on individual computers requires a great deal of administrative effort. Because of this you will usually deploy the IPSec policies by using the Group Policies in Active Directory. To create a policy to be used for Active Directory, follow the steps outlined below:

1. Create a custom MMC with the **IP Security Policy Management** snap-in. When installing the snap-in, the focus of the policy can be set to the local computer, another computer, or a domain. Choose the domain option.

2. Using this MMC, you can configure the IPSec policy in many different ways. You may want to implement one of the three built-in options. Or you can customize one of the default options or apply a customized option that you have created. For example, the policy could be configured to:

   a. Use IPSec only for certain kinds of traffic. The filter can be set to use IPSec for all IP traffic or only certain protocols and port numbers.

b. Use IPSec only when communicating with certain computers. The filter can be set to use IPSec only when the traffic is intended for a particular IP address.

c. Use IPSec only for LAN or Remote Access connections.

d. Control how frequently new keys must be generated and what kinds of security methods to use.

   If the MMC snap-in is configured to edit the IPSec policy for the domain, any configuration changes will automatically change the domain security policy.

3. To deploy the domain security policy, open the **Domain Security Policy** MMC from the Administrative tools menu. The IP Security Policies on Active Directory is listed as one of the components in the Domain Security Policy.

4. Right-click the policy to be assigned to the domain, for example, Client (Respond Only), and click **Assign**. The policy will now be enforced for the domain. Setting the policy here will override any local policy set on any computer that is part of a domain.

IPSec policies can be assigned at the site, domain, or OU level. To apply an IPSec policy to a site or an organizational unit, create a group policy object for the specific container and edit the Group Policy template to configure the IPSec settings. In a workgroup environment, a set of local IPSec policies can be exported to an .ipsec file. This file can then be imported into other machines within the workgroup. To export or import the policies, right-click the IP Security Policies node on the left pane of the MMC, click All Tasks, and click Export or Import (as shown in Figure 7-16).

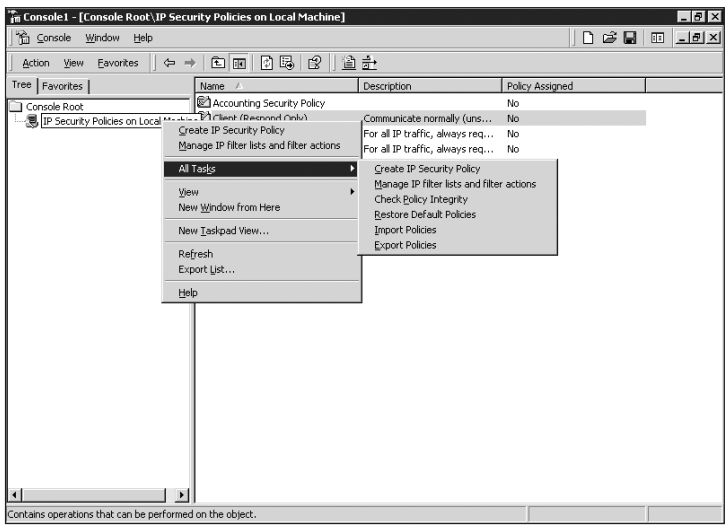

Figure 7-16 Exporting IP Security policies

Planning Best Practices

- If you require SMB signing, be sure to implement it at both the client and the server. This will insure that proper security is in place for all network communication.
- If the network includes operating systems that do not support SMB, configure SMB signing on the servers to request signed messages. If you require signed messages, then clients that cannot support SMB signing will not be able to connect to the server.
- Create an organizational unit and place all servers that require the same SMB signing policy into the OU. Assign the security template containing the SMB configuration settings to the organizational unit.
- Because of the potential for performance degradation on file servers if all traffic must be protected using SMB signing, you will need to plan the implementation of SMB signing carefully. You may want to configure SMB signing on all the file servers, but enable SMB signing on only the client computer that may be sending highly confidential information to the file server. Configuring the computers in this way means that the server will attempt to set up SMB signing with all clients, but it will be enabled only on the client connections from the computers that are also enabled. This configuration will minimize the performance degradation on the server, while still protecting all the highly confidential information.
- Use Authentication Headers within IPSec to insure that only authenticated computers can participate in data transmissions.
- If Network Address Translation (NAT) is being used behind a firewall, and IPSec is needed to protect data up to the firewall, implement IPSec in tunnel mode to allow protection of data up to the NAT server point. Another option is to implement a dual-homed Tunnel Server at each location to bypass the firewall.
- The configuration procedures in this chapter have all dealt with configuring IPSec in transport mode. Chapter 9, "Securing Access Between Corporate Locations" will cover the concepts and procedures for configuring IPSec in tunnel mode.
- Place all computer accounts that require the same IP Sec configurations within the same organizational unit, and then use group policies to configure the IPSec settings.
- You can troubleshoot IPSec communication by using the ping utility or by using the IPSec monitor (ipsecmon.exe).

- To enable detailed debugging of an IPSec connection, enable Oakley logs by adding the setting, EnableLogging value to 1 (REG_DWORD) to the Registry key:
  HKLM\System\CurrentControlSet\Services\PolicyAgent\Oakley
  The Oakley logs are stored in the %systemroot%\debug folder and contain very detailed and often obscure information. Use this option only as a last resort and be prepared to spend a significant amount of effort in researching the log information.

CHAPTER SUMMARY

- Server Message Block (SMB) signing allows mutual authentication and message authentication to occur between a server and a client. SMB signing is supported by most Windows operating systems such as Windows 98, NT, and 2000, but is not supported on Windows 95 clients.
- SMB signing is configured by editing a Registry setting within Windows. The Registry edit can be performed manually by importing a Registry file or, if using Windows 2000 machines, through group policy.
- IPSec consists of two protocols that can be used independently or together to protect data. The Authentication Header Protocol (AH) provides data authentication, integrity, and anti-replay protection for the data transmitted over the network connection. Encapsulating Security Payload (ESP), similar to Authentication Headers, provides authentication, integrity, and anti-replay protection, but also provides data encryption capabilities.
- Windows 2000 implements IPSec by utilizing various components such as the IPSec Driver, Internet Key Exchange (IKE), and the IPSec Policy Agent Service.
- There are three main steps in creating an IP Security Policy. The first is to create or edit policy filters. The second step is to define which actions will take place when a transmission matches an assigned filter. The third step is to decide upon the type of authentication that will take place before IP Security negotiations occur.
- IPSec policies can be deployed using the TCP/IP advanced properties on standalone machines, or by assigning the policy to a site, domain, or organizational unit using group policies within Active Directory.

KEY TERMS

Server Message Block (SMB) — (Also known as Common Internet File System) A protocol used between computers to share resources such as files, printers, and communication connections, including named pipes and mail slots.

SMB signing — Refers to the option to digitally sign each message block that is sent to or from a server and client. This digital signature authenticates both computers in the network communication and provides data integrity.

IP Security (IPSec) — A protocol used for data authentication and encryption over a TCP/IP network.

Authentication Header Protocol (AH) — A part of IPSec that provides data authentication, integrity, and anti-replay protection for the data transmitted over the connection.

Encapsulating Security Payload (ESP) — A second protocol used in IPSec that provides data authentication, integrity, and anti-replay protection, as well as encrypts the data transmitted over the connection.

Transport mode — An IPSec mode implemented when communications need to be encrypted from an originating computer through to a target computer.

Tunnel mode — An IPSec mode where the transmitted data is protected only between two points in a communication channel, thus forming a protected "tunnel" for part of the channel.

Internet Key Exchange (IKE) — An IPSec component that manages Security Associations and manages the generation and exchange of the keys between the two systems.

IPSec driver — Receives the filter list from the IPSec Policy configured on the machine. The IPSec driver also is in charge of the IKE to make sure that the key exchange process is taking place between the two machines.

Security Association (SA) — Defines the authentication and encryption process for the IPSec communication.

Review Questions

1. Which of the following are benefits of IPSec in Windows 2000?
   a. data transmitted across the network is secure
   b. applications need not be aware that IPSec is being used
   c. the client and server negotiate the highest level of security
   d. all of the above
2. Which component of IPSec security encrypts transmitted data between two Windows 2000 computers?
   a. Respond
   b. Request Security
   c. Encapsulating Security Payload (ESP)
   d. Authentication Header (AH)

3. You want to configure your Windows 2000 servers to always attempt to use IPSec when a client connects, but to still accept connections from clients that do not support IPSec. What IPSec configuration option should you use?
   a. Secure Server (Require Security)
   b. Server (Request Security)
   c. Client (Respond Only)
4. One of the benefits of IPSec is mutual authentication. What is mutual authentication?
   a. a client provides identifying information to a server
   b. a server provides identifying information to a client
   c. a client and server provide identifying information to each other
5. Which clients can take advantage of SMB signing?
   a. Windows 2000 Professional
   b. Windows 95
   c. Windows 98
   d. Windows 4.0 Professional (SP 6a)
6. Which technology can be used with Windows 2000 and Windows NT to ensure data integrity for all network transactions?
   a. IPSec AH
   b. IPSec ESP
   c. SMB signing
   d. DES
7. What tool is used to enable SMB signing on a Windows 2000 server?
   a. Routing and Remote Access
   b. Active Directory Users and Computers
   c. Computer Management
   d. Regedit.exe
8. Network response times will be slower if SMB signing is used. True or false?
9. Which encryption technology would you choose to specify the highest level of encryption possible with IPSec ESP?
   a. DES
   b. 3DES
   c. 40-bit DES
   d. 128-bit SSL

10. Which of the following filtering options can you use to configure IPSec filters?
    a. Source or Destination IP address
    b. IPX network number
    c. Protocol Type
    d. Source or destination port number
11. Which IPSec authentication method is the easiest to implement if both computers are part of the same Active Directory forest?
    a. certificate-based authentication
    b. preshared key authentication
    c. Kerberos version 5 authentication
    d. all are equally easy
12. Which IPSec authentication method is the most secure to implement if both computers are in different Active Directory trees and have access to the Internet?
    a. Certificate-based authentication
    b. Preshared key authentication
    c. Kerberos version 5 authentication
    d. all are equally secure
13. If your network has very high security requirements and you would like all of your network traffic to be encrypted with IPSec, which security policy would you implement on your servers?
    a. Client (Respond Only)
    b. Secure Server (Require Security)
    c. Server (Request Security)
14. After implementing the security policy Server (Request Security) on a Windows 2000 server, which operating systems will be able to communicate with the server? Select all that apply.
    a. Windows 2000 Professional
    b. Windows NT 4.0
    c. Windows 95
    d. Windows 3.11
15. After implementing the security policy Secure Server (Require Security) on a Windows 2000 server, which operating systems will be able to communicate with the server?
    a. Windows 2000 Professional
    b. Windows NT 4.0
    c. Windows 95
    d. Macintosh

16. Which MMC snap-in is used to create IPSec policies for the domain?
    a. Routing and Remote Access
    b. Active Directory Users and Computers
    c. Computer Management
    d. IP Security Policy Management
17. IPSec can be used to set up a secure tunnel for communication across the Internet without using L2TP. True or false?
18. You would like to use IPSec to encrypt only the traffic sent between the workstations and servers in the Accounting department. How could you configure this with the least amount of administrative effort?
    a. edit the Registry on all the computers
    b. set the IPSec policy on each computer to Require Security
    c. move all the accounting computers into an OU and configure the Group Policy for that OU
    d. configure the Domain Security Policy to Require Security

HANDS-ON PROJECTS

Project 7-1

In this hands-on activity, you will configure the server to request Server Message Block signing.

To configure SMB signing for all Domain Controllers:

1. Log on to your Windows 2000 computer as an administrator.
2. Open **Active Directory Users and Computers** from the Administrative Tools menu.
3. Right-click the **Domain Controllers** OU. Choose **Properties**.
4. Click the **Group Policy** tab.
5. Click **New** to create a new Group Policy object. Call the policy **SMB Policy**.
6. Select **SMB policy** and click **Edit**.
7. Under the Computer Configuration node, browse to the **Windows Settings\Security Settings\Local Policies\Security Options** section.
8. Scroll to and double-click the **Digitally sign server communication (when Possible)** configuration.
9. Click the check box next to **Define this policy setting** and then click **Enabled**.
10. Close all windows and restart the computer.

Project 7-2

In this hands-on activity, you will create an IPSec policy filter that will only apply to a machine with the pre-configured IP address of 10.0.0.15

To create an IPSec policy filter:

1. Log on to your Windows 2000 computer as an administrator.
2. Open **Local Security Policy** from the Administrative Tools menu.
3. Click the **IP Security Policies on Local Machine** node in the left pane. The three default IPSec polices will appear in the right-most details pane.
4. Right-click **IP Security Policies on Local Machine** and click **Manage IP filter lists and filter actions**.
5. Click the **Add** button and type **Connection to Finance Server** as the Name.
6. Turn off the **Use Add Wizard** by deselecting the check box. Click the **Add** button. The Filter Properties will appear.
7. Click the drop-down menu under **Destination Address**, and choose **A specific IP Address**. Add the IP address of **10.0.0.15**, which represents the Finance Server.
8. Click **Mirrored** to ensure that data is encrypted both ways.
9. Click the **Description** tab and add a description on what this filter does. Click **OK** and then **Close** to return to the **Manage IP filter lists and filter actions** dialog box.
10. Click the **Manage Filter Actions** tab. These are the default actions that can be applied to a filter. The defaults are sufficient for our purpose. Click the **Close** button.
11. Continue to the next project.

Project 7-3

In this hands-on project, you will create a new IPSec policy that will require all communications to be secure between your machine and the Finance server.

To create a new IPSec policy:

1. Right-click **IP Security Polices on Local Machine** and choose **Create IP Security Policy**.
2. The IP Security Policy Wizard appears. Click the **Next** Button.
3. Name the policy **Finance Server IPSec Policy**. Click **Next**.
4. Turn off the default response rule, as it will not be needed for our policy. Click **Next** and then click **Finish**. The New policy properties dialog box will appear.
5. Click the **Add** button to add a new security rule to the policy.
6. On the IP Filter list tab, choose the **Connection to Finance Server** filter.

7. On the Filter action tab, click **Require Security**. The rest of the tabs can be left at the default settings.
8. Click **OK** and then click **Close**.
9. Close all windows and log off.

Project 7-4

In this hands-on activity, you will assign the Finance Server IPSec Policy to your server to ensure that all communication between your server and the Finance server is secure.

To assign an IPSec policy to a computer:

1. With an administrator account, log on to your Windows 2000 computer.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Local Security Policy**.
3. Click **IP Security Policies on Local Machine**.
4. Right-click **Finance Server IPSec Policy** and click **Assign**.
5. What program can you run to monitor and troubleshoot IPSec communication?
6. Close all windows and log off.

CASE PROJECTS

Case Project 7-1

One of the managers at Southdale Property Management read something about packet sniffers on the Internet and is now concerned about the security of the information that is being sent on the network at the company. He is especially concerned with the information that is being sent to the Internet in the form of e-mail messages, but is also concerned about some confidential information that is being sent from the managers' and accountants' computers to the file and print server. What would you advise this manager to do?

Case Project 7-2

One of the security concerns at Fleetwood Credit Union is the security of network packets. On a normal day, Fleetwood Credit Union performs several thousand financial transactions worth millions of dollars. In most cases the data is entered at a teller or financial consultant's computer and then transmitted across the network to a Windows 2000 server at head office. If someone was able to capture the packets on the network, or implement a man-in-the-middle attack, the damage in terms of financial cost and reputation could be very serious. The management would also like to make sure that all traffic on the frame relay lines is secure, just in case someone breaks into the ISP's network. How can you ensure the security of the data?